

under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

26. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

27. While Parnas, Correia, and others have been publicly indicted with respect to separate charges, and there has been some public reporting about the existence of an investigation into the removal of Ambassador [REDACTED] the scope and focus of this aspect of the criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert criminal targets to the scope and focus of the investigation, causing them to destroy evidence, tamper with witnesses, or otherwise seriously jeopardize the

investigation. Specifically, from my experience investigating public corruption offenses, I know that individuals who participate in offenses such as the Subject Offenses may communicate about known government investigations and tailor their stories to be consistent, and tamper with or hide potential evidence. Accordingly, premature disclosure of the scope of this investigation would undermine efforts to obtain truthful statements from relevant witnesses, and could lead to witness tampering and/or obstruction of justice. In addition, if the subjects of this investigation were alerted to the existence of a criminal investigation, it may prompt them to delete electronic records, including in e-mail accounts or other electronic media not presently known to the government. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized.

28. Additionally, while the Subject Accounts are registered to an enterprise domain (fraudguarantee.com), there is no representative of the enterprise that could be notified without seriously jeopardizing the investigation. Indeed, as described above, the subscribers of the Subject Accounts are the CEO and COO of the enterprise, the enterprise itself appears to be an instrumentality of the fraudulent scheme, and there is no known employee of the enterprise or a legal representative that could be notified without jeopardizing the investigation. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person, including any representative of the enterprise domain fraudguarantee.com, of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

29. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as


need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

30. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.



Sworn to before me this
12th day of December, 2019


HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19 MAG 11651

In the Matter of a Warrant for All
Content and Other Information
Associated with the Email Accounts
[REDACTED] and
[REDACTED]
Maintained at Premises Controlled by
Google, LLC, USAO Reference No.
[REDACTED]

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, LLC ("Provider")

Federal Bureau of Investigation and United States Attorney's Office for the Southern
District of New York


1. **Warrant.** Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED] and [REDACTED] maintained at premises controlled by Google, LLC, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, and/or tampering with potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person, including but not limited to a representative of the enterprise domain, for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Dec. 12, 2019 3:03 PM
Date Issued Time Issued


HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google, LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts [REDACTED] and [REDACTED] (the "Subject Accounts"). The Provider is directed to produce the information described below associated with the Subject Accounts, limited to content created, sent, or received on or after September 1, 2013 through the date of this warrant.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts (subject to the time period limitation set forth above):

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Google Drive Content.* All Google Drive records associated with the Subject Accounts, including all documents and other records stored on the Google Drive accounts.

f. *Google Docs.* All Google Docs records associated with the Subject Accounts, including all documents created or stored in Google Docs.

g. *Google Calendar.* All calendar entries and records associated with the Subject Accounts.

h. *Location History.* All location records associated with the Subject Accounts.

i. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by Cookie, email account, phone number, Google Account ID, Android ID, or other account or device identifier.

j. *Device Information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber

Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the Subject Accounts;

k. *Android Services*. All records relating to Android services associated with the Subject Accounts.

l. *Preserved or backup records*. Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the “Subject Offenses”), including the following:

- a. Evidence relating to, including communications with, Rudolph Giuliani, [REDACTED] and any actual or potential investors, members, or partners of Fraud Guarantee;
- b. Evidence relating to Fraud Guarantee’s plans, finances, assets, and operations, or lack thereof, including any corporate books and records;
- c. Evidence relating to Fraud Guarantee’s actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;
- d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;
- e. Evidence relating to Fraud Guarantee’s members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to the nature and extent of Rudolph Giuliani's and [REDACTED] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [REDACTED] and whether or not such efforts benefited Fraud Guarantee;

g. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

h. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

i. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

j. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

k. Passwords or other information needed to access user's online accounts.

Exhibit 1
